UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,238	12/22/2000	David W. Grawrock	42390P9257	9482

8791 7590 09/20/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,238	GRAWROCK	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-9 and 11-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-9 and 11-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 06/28/2005. Claims 3-6, 9, 12, 15, 20 and 25 have been amended; claim 10 has been cancelled.

Response to Arguments

2. Applicant's arguments filed 06/28/2005 with respect to claims 3 and 9 have been considered but are not persuasive. Applicant's amendments have necessitated a new search and new grounds of rejection.

3. Applicant's arguments filed 06/28/2005 with respect to claims 15, 20 and 25 have been fully considered but they are not persuasive. Regarding the rejection of claim 15, Applicant argues that Davis (5,818,939) does not disclose an asymmetric key generation unit contained within the package to generate a long-term value a short term value, the long term value generated upon detecting an initial power-up sequence based on information provided by the ICH (page 10, last paragraph). Davis discloses an asymmetric key generation unit contained within the package to generate a long-term value (i.e., a shared secret key) and a short-term value (i.e., a session key), the long-term value generated upon detecting an initial power-up sequence when the TPM communicates with the chipset (col. 5, lines 24-44). Regarding the rejection of claims 20 and 25, Applicant argues that Davis does not disclose that a long-term value is generated in response to an initial non-repeating event (page 11, 4th paragraph). Davis

discloses that a shared secret key is generated in response to an initial power-up during manufacture (col. 5, lines 24-35).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 2-7, 9, 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (5,819,939) in view of Menezes ("Handbook of Applied Cryptography", Section 12.3) and Levy et al (6,212,633).

Regarding claims 3, 2 and 4-5, Davis discloses a method in which a chipset communicates with a cryptographic unit when both devices are powered up during manufacture, the cryptographic unit then generates a shared secret key which is a long-term value, and stores the shared secret key in a protected internal memory. Davis further discloses that the cryptographic unit also generates a session key in response to a communication session which is a periodic event, the session key being a short term value and also a secret value (fig. 4; col. 5, lines 25-44).

Davis does not disclose that the session key is a combination of the shared secret key and a short-term value. Menezes discloses a first entity, entity B, that generates a short-term value and then generates a secret value that is a combination of a shared long-term value, and a short-term value (p. 499, 2nd par., "In the other

techniques ... and key derivation"; section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis method such that the secret value is a combination of both the long-term value and a short-term value, as taught by Menezes. The motivation for doing so would have been a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd par).

Davis does not disclose that the periodic event being a power-up sequence. Levy discloses that new session keys are generated in response to a power-up sequence (col. 9, lines 46-59; col. 16, lines 54-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis method further to generate the secret value in response to the power-up sequence, as taught by Levy. Accordingly the short-term value is also generated in response to the power-up sequence. The motivation for doing so would have been that the encryption scheme is changed on a regular basis, thereby heightening the security for the interface.

Regarding claim 6, Menezes further discloses transmitting a second command from a second entity, entity A, to the first entity and generating the short-term value within the first entity in response to the second command (page 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis method to transmit a second command from a second entity to the first entity and generate the short-term value within the first entity in response to the second command, as taught by Menezes. Please refer to motivation recited for

generating a secret value within the first device, the secret value being a combination of both the long-term value and a short-term value as taught by Menezes in claim 3.

Regarding claim 7, Menezes further discloses transmitting the short-term value to a second entity prior to producing the secret value (page 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis method to transmit the short-term value to the second device prior to producing the secret value, as taught by Menezes. Please refer to motivation recited for generating a secret value within the first device, the secret value being a combination of both the long-term value and a short-term value as taught by Menezes in claim 3.

Regarding claims 9 and 12-13, Davis discloses a method comprising: generating a shared secret key, which is a long-term value, within a cryptographic unit, the shared secret key generated upon detecting an initial power-up of a chipset during manufacture; permanently storing the long-term value within a protected area of an internal memory; providing the long-term value to a second device communicatively coupled to the chipset; generating a session key for each communication session which is a periodic event, the session key being a short term value and also a secret value. Davis does not disclose the short-term value being modified after each power up sequence; providing the short-term value to the second device; and generating a secret value within the first device and the second device, the secret value being a combination of both the long-term value and the short-term value.

Menezes discloses a method for deriving a session key for each communications session between two entities using a long-term secret shared by the entities, the method comprising: generating a short-term value within a first entity, entity B, the short-term value being modified after each periodic event; providing the short-term value to the second device; and generating a session key, which meets the limitation of a secret value, within the first and second entities, the session key being a combination of both the long-term value and the short-term value (p. 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis method to include the steps of generating a short-term value within the first device, the short-term value being modified after each periodic event; providing the short-term value to the second device; and generating a session key within the first device and the second device, the session key being a combination of both the long-term value and the short-term value, as taught by Menezes. The use of session keys would limit available ciphertext (under a fixed key) for cryptanalyst attack (p. 494, 1st par.).

Levy discloses that new session keys, which meet the limitation of secret values, are generated in response to a power-up sequence (col. 9, lines 46-59; col. 16, lines 54-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis method further to generate the secret value in response to the power-up sequence, as taught by Levy. Accordingly the short-term value is also generated in response to the power-up sequence. The motivation for

doing so would have been that the encryption scheme is changed on a regular basis, thereby heightening the security for the interface.

6. Claims 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes and Levy as applied to claims 3 and 9 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Menezes discloses that the combination of claim 3 is a result produced by performing a hash operation on both the data and the short-term value. However, Menezes does not disclose that the hash operation is performed successively. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claims 3 and 9 such that that the hash operation is performed successively, as taught by Menezes, in order to slow down attacks.

7. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes and Levy as applied to claim 9 above, and further in view of Burns ("INTEL: Intel introduces new chipset for intel Pentium III processor-based performance PCs"). Davis further discloses a cryptographic unit which meets the limitation of a trusted platform module (fig. 4). Davis does not disclose an input/output control hub (ICH). Burns discloses a chipset comprising an ICH ("This revolutionary chipset architecture ... and a Firmware Hub"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis method further

such that the second device is an ICH, as taught by Burns. The ICH includes an Alert on LAN feature that allows a non-booting system to send a status update to the network administrator even when the microprocessor is not present.

8. Claims 15-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('939) in view of Menezes ("Handbook of Applied Cryptography", Section 12.3) and Burns.

Regarding claims 15-16, Davis discloses a platform comprising: a link (fig. 4, element 330); a chipset coupled to the link (fig. 4, element 315); and a cryptographic device, which meets the limitation of a trusted platform module (TPM), coupled to the link (fig. 4, element 335), the cryptographic coprocessor including a package (fig. 4, element 335), an asymmetric key generation unit contained within the packet to generate a shared secret key, which meets the limitation of a long term value (col. 5, lines 24-44; col. 6, lines 57-65), the shared secret key generated upon detecting an initial power-up sequence based on information provided by the chipset; and an internal memory contained within the package, the internal memory to permanently store the shared secret key (fig. 4, element 610) and to temporarily store a session key, which meets the limitation of a secret value (col. 6, lines 25-28).

Davis does not disclose an input/output control hub (ICH). Burns discloses a chipset comprising an ICH ("This revolutionary chipset architecture ... and a Firmware Hub"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis platform to use a chipset comprising an ICH, as

taught by Burns. The ICH includes an Alert on LAN feature that allows a non-booting system to send a status update to the network administrator even when the microprocessor is not present.

Davis does not disclose that the asymmetric key generation unit generates a short-term value and the session key being a combination of the shared secret key and the short-term value. Menezes discloses a device that has a long-term shared secret key (p. 497, "Point-to-point key update ... a priori by two parties A and B"); and the device generates a short-term value and a session key, which meets the limitation of a secret value, the session key being a combination of the shared secret key and the short-term value (p. 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis platform such that the asymmetric key generation unit generates a short-term value and a secret value being a combination of the shared secret key and the short-term value, as taught by Menezes. The motivation for doing so would have been that a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd par.).

Regarding claim 18, Davis further discloses that the asymmetric key generation unit includes a number generator (fig. 4, element 620).

9. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('939), Menezes and Burns as applied to claim 16 above, and further in view of Davis (5,949,881). Davis ('939) discloses that the cryptographic device transmits the shared

secret key to the chipset over the link during manufacture of the platform (col. 5, lines 24-36; col. 6, lines 6-30); however, Davis does not disclose that the cryptographic device transmits the shared secret key to the ICH over the link during manufacture of the platform and transmits the short term value to the ICH over the link in response to a power-up sequence by the platform. Davis ('881) discloses a platform comprising a cryptographic device and an I/O controller, which meets the limitation of an ICH (fig. 1, elements 130 and 151). Davis further discloses that the cryptographic device and the I/O controller share a secret key (fig. 1; col. 3, lines 25-29), and that the cryptographic device generates and uses a session key, in addition to the symmetric key, to authenticate and activate the platform in response to a power-up sequence by the platform (fig. 2; col. 3, lines 13-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the platform of claim 16 such that the cryptographic device generates and uses a session key, in addition to the symmetric key, to authenticate and activate the platform in response to a power-up sequence by the platform, as disclosed by Davis in reference '881. Accordingly, the cryptographic device needs to transmit the long-term value to the ICH over the link during manufacture of the platform and transmit the short-term value to the ICH over the link in response to a power-up sequence by the platform. The motivation for doing so would have been to reduce the value of a laptop computer in the event of its theft or loss and thus, in effect, would deter such theft and encourage its return in the event of loss (col. 1, lines 53-57).

10. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, Menezes and Burns as applied to claim 15 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Menezes (p. 499, section 12.20) discloses that the secret value is a result produced by performing a hash operation on both the long-term value and the short-term value. However, Menezes does not disclose that the hash operation is performed successively. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 15 such that that the hash operation is performed successively, as taught by Menezes, in order to slow down attacks.

1. Claims 20, 22-23, 25-26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('939) in view of Menezes (Section 12.3).

Regarding claims 20, 22, 25-26 and 28, Davis discloses a device comprising: an internal memory (fig. 4, element 610); an asymmetric key generation unit to generate, in response to an initial power up sequence of the device when in communication with another device during manufacture, a unique long-term value for permanent storage in a protected area of the internal memory (col. 5, lines 24-44; col. 6, lines 57-65). Davis further discloses that the asymmetric key generation unit generates a session key, which meets the limitation of a secret value; however, Davis does not disclose that the asymmetric key generation unit generates, in response to a periodic event, a short-term value for storage in the internal memory and a cryptographic engine to produce the

session key by combining both the long-term value and the short-term value. Menezes discloses a key generation unit for deriving a session key, which meets the limitation of a secret value, by generating, in response to a periodic event, a short-term value for storage in the internal memory; and a cryptographic engine to produce the session key by combining both the long-term value and the short-term value (p. 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis device such that the asymmetric key generation unit generates, in response to a periodic event, a short-term value for storage in the internal memory and a cryptographic engine to produce a secret value by combining both the long-term value and the short-term value, as taught by Menezes. The motivation for doing so would have been that a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd paragraph).

Regarding claim 23, Davis further discloses that the internal memory includes a non-volatile memory (fig. 4, element 610) and a volatile memory (fig. 4, element 615).

11. Claims 21 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes as applied to claims 20 and 25 above, and further in view of Levy. Davis and Menezes do not disclose that the periodic event includes a power-up sequence. Levy discloses that new session keys, which meet the limitation of secret values, are generated in response to a power-up sequence (col. 9, lines 46-59; col. 16, lines 54-62). It would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the Davis method further to generate the secret value in response to the power-up sequence, as taught by Levy. Accordingly the short-term value is also generated in response to the power-up sequence. The motivation for doing so would have been that the encryption scheme is changed on a regular basis, thereby heightening the security for the interface.

12. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes as applied to claim 20 above, and further in view of Menezes (Section 10.2). Menezes (p. 499, section 12.20) discloses that the secret value is a result produced by performing a hash operation on both the long-term value and the short-term value. However, Menezes does not disclose that the hash operation is performed successively. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 20 such that that the hash operation is performed successively, as taught by Menezes, in order to slow down attacks.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,680,131 to Utz

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
9/17/05

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100